

Appl. No. 10/531,753
Amdt. Dated June 1, 2009
Reply to Office action of March 31, 2009
Attorney Docket No. P17299-US1
EUS/GJ/P/09-1127

RECEIVED
CENTRAL FAX CENTER
JUN 01 2009

Amendments to the Claims:

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1-12. (Cancelled)

13. (Previously Presented) A method for preventing illegitimate use of an Internet Protocol (IP) address by a subscriber device in an IP network, the network including a switch node and at least one DHCP server, said subscriber device in communication with the switch node, the method including the steps of:

creating a list of trusted ones of the DHCP servers in said switch node;

transmitting by the subscriber device a DHCP request message for an IP address;

receiving a reply message by said switch node which carries an assigned subscriber IP address;

analysing the reply message by said switch node to be a DHCP message and having a source address from one of the trusted DHCP servers;

updating a filter dynamically in the switch node, the filter storing an identification of the subscriber device and the assigned subscriber IP address;

transmitting a frame from the subscriber device using a source IP address;

comparing in the filter said source IP address with the stored subscriber IP address;
and,

discarding said frame when said source IP address differs from the stored subscriber IP address.

14. (Previously Presented) The method according to claim 13, further comprising the step of storing in the filter a subscriber MAC address, a subscriber physical port number, a subscriber virtual LAN identity and a lease time interval for the assigned subscriber IP address.

Appl. No. 10/531,753
Amdt. Dated June 1, 2009
Reply to Office action of March 31, 2009
Attorney Docket No. P17299-US1
EUS/GJ/P/09-1127

15. (Previously Presented) The method according to claim 13, wherein the subscriber IP address is statically assigned and handled by the DHCP servers.
16. (Previously Presented) The method according to claim 14, the method including deleting the subscriber identification and the corresponding assigned subscriber IP address from the filter when the lease time interval is out.
17. (Previously Presented) The method according to claim 13, the method further comprising the steps of:
- counting a number of attempts (n) from the subscriber to use an illegitimate IP address;
 - comparing the number (n) of the attempts with a threshold number (N);
 - sending a warning signal when the number of attempts exceeds a threshold criteria.
18. (Previously Presented) A switch node in an Internet Protocol (IP) network adapted to prevent illegitimate use of an IP address by a subscriber device, the switch node including:
- at least one port for communication with a subscriber device;
 - an uplink port for communication with DHCP servers in the network; and,
 - a filter device having a list of trusted ones of the DHCP servers, the filter device being associated with the ports; wherein the switch node is operative to:
 - receive a subscriber IP address request message from a subscriber device, analyse it to be a DHCP request message and transmit it on the uplink port;
 - receive a reply message on the uplink port, analyse it to be a DHCP reply message having a source IP address from one of the trusted DHCP servers on the list;
 - dynamically update the filter with an identification of the subscriber device and a corresponding assigned subscriber IP address contained in the DHCP reply message;
 - receive a frame with a source IP address from a subscriber device;
 - compare in the filter said source IP address with the stored subscriber IP address for the subscriber device; and,

Appl. No. 10/531,753
Amdt. Dated June 1, 2009
Reply to Office action of March 31, 2009
Attorney Docket No. P17299-US1
EUS/GJ/P/09-1127

to discard said frame when said source IP address differs from the stored subscriber IP address.

19. (Previously Presented) The switch node according to claim 18, wherein the switch node is further operative to store in the filter a subscriber MAC address, a subscriber physical port number, a subscriber virtual LAN identity and a lease time interval for the assigned subscriber IP address.

20. (Previously Presented) The switch node according to claim 18, wherein the subscriber IP address comprises a statically assigned address which is handled by the DHCP servers.

21. (Previously Presented) The switch node according to claim 19, wherein the switch node is further operative to delete the subscriber identification and the corresponding assigned subscriber IP address from the filter when the lease time interval ~~is out~~ expires.

22. (Previously Presented) The switch node according to claim 18, wherein the filter comprises a counter operative to count a number (n) of discarded frames on the subscriber port, to compare the number (n) of the discarded frames with a threshold number (N), and to send a warning signal when the number of discarded frames exceeds a threshold criterion.

* * *